A DYNAMICAL PROPERTY UNIQUE TO THE LUCAS SEQUENCE

YASH PURI AND THOMAS WARD

School of Mathematics, University of East Anglia, Norwich, NR4 7TJ, U.K.

1. Introduction

A *dynamical system* is taken here to mean a homeomorphism

$$f : X \to X$$

of a compact metric space X (though the observations here apply equally well to any bijection on a set). The number of points with period n under f is

$$\mathrm{Per}_n(f) = \#\{x \in X \mid f^n x = x\},$$

and the number of points with least period n under f is

$$\mathrm{LPer}_n(f) = \#\{x \in X \mid \#\{f^k x\}_{k\in\mathbb{Z}} = n\}.$$

There are two basic properties that the resulting sequences $(\mathrm{Per}_n(f))$ and $(\mathrm{LPer}_n(f))$ must satisfy if they are finite. Firstly, the set of points with period n is the disjoint union of the sets of points with least period

Date: February 1, 2008.

The first author gratefully acknowledges the support of E.P.S.R.C. grant 96001638.

d for each divisor d of n, so

$$\mathrm{Per}_n(f) = \sum_{d|n} \mathrm{LPer}_d(f). \tag{1}$$

Secondly, if x is a point with least period d, then the d distinct points $x, f(x), f^2(x), \dots, f^{d-1}(x)$ are all points with least period d, so

$$0 \le \mathrm{LPer}_d(f) \equiv 0 \bmod d. \tag{2}$$

Equation (1) may be inverted via the Möbius inversion formula to give

$$\mathrm{LPer}_n(f) = \sum_{d|n} \mu(n/d)\mathrm{Per}_d(f),$$

where $\mu(\cdot)$ is the Möbius function defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has a squared factor, and} \\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes.} \end{cases}$$

A short proof of the inversion formula may be found in [4, Section 2.6].

Equation (2) therefore implies that

$$0 \le \sum_{d|n} \mu(n/d)\mathrm{Per}_d(f) \equiv 0 \bmod n. \tag{3}$$

Indeed, equation (3) is the only condition on periodic points in dynamical systems: define a given sequence of non-negative integers (U_n) to be *exactly realizable* if there is a dynamical system $f : X \to X$ with $U_n = \mathrm{Per}_n(f)$ for all $n \ge 1$. Then (U_n) is exactly realizable if and only

if

$$0 \le \sum_{d|n} \mu(n/d) U_d \equiv 0 \bmod n \text{ for all } n \ge 1,$$

since the realizing map may be constructed as an infinite permutation using the quantities $\frac{1}{n}\sum_{d|n} \mu(n/d)U_d$ to determine the number of cycles of length n.

Our purpose here is to study sequences of the form

$$U_{n+2} = U_{n+1} + U_n, n \ge 1, \quad U_1 = a, U_2 = b, \quad a, b > 0 \tag{4}$$

with the distinguished Fibonacci sequence denoted (F_n), so

$$U_n = aF_{n-2} + bF_{n-1} \text{ for } n \ge 3. \tag{5}$$

Theorem 1. *The sequence* (U_n) *defined by* (4) *is exactly realizable if and only if* $b = 3a$.

This result has two parts: the *existence* of the realizing dynamical system is described first, which gives many modular corollaries concerning the Fibonacci numbers. One of these is used in the *obstruction* part of the result later. The realizing system is (essentially) a very familiar and well-known system, the *golden-mean shift*.

The fact that (up to scalar multiples) the Lucas sequence (L_n) is the only exactly realizable sequence satisfying the Fibonacci recurrence relation to some extent explains the familiar observation that (L_n) satisfies a great array of congruences.

Throughout, n will denote a positive integer and p, q distinct prime numbers.

2. Existence

An excellent introduction to the family of dynamical systems from which the example comes is the recent book by Lind and Marcus [2]. Let

$$X = \left\{ \mathbf{x} = (x_k) \in \{0,1\}^{\mathbb{Z}} \mid x_k = 1 \implies x_{k+1} = 0 \text{ for all } k \in \mathbb{Z} \right\}.$$

The set X is a compact metric space in a natural metric (see [2, Chapter 6] for the details). The set X may also be thought of as the set of all (infinitely long in both past and future) itineraries of a journey involving two locations (0 and 1), obeying the rule that from 1 you must travel to 0, and from 0 you must travel to either 0 or 1. Define the homeomorphism $f : X \to X$ to be the *left shift*,

$$(f(\mathbf{x}))_k = x_{k+1} \text{ for all } k \in \mathbb{Z}.$$

The dynamical system $f : X \to X$ is a simple example of a *subshift of finite type*. It is easy to check that the number of points of period n under this map is given by

$$\mathrm{Per}_n(f) = \mathrm{trace}\left(A^n\right) \tag{6}$$

where $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ (see [2, Proposition 2.2.12]; the $0-1$ entries in the matrix A correspond to the allowed transitions $0 \to 0$ or 1; $1 \to 0$ in

the elements of X thought of as infinitely long journeys in a graph with vertices 0 and 1).

Lemma 2. *If $b = 3a$ in (4), then the corresponding sequence is exactly realizable.*

Proof. A simple induction argument shows that (6) reduces to $\mathrm{Per}_n(f) = L_n$ for $n \geq 1$, so the case $a = 1$ is realized using the golden mean shift itself. For the general case, let $\bar{X} = X \times B$ where B is a set with a elements, and define $\bar{f} : \bar{X} \to \bar{X}$ by $\bar{f}(\mathbf{x}, y) = (f(\mathbf{x}), y)$. Then $\mathrm{Per}_n(\bar{f}) = a \times \mathrm{Per}_n(f)$ so we are done. □

The relation (3) must as a result hold for (L_n).

Corollary 3. $\sum_{d|n} \mu(n/d) L_d \equiv 0$ *mod n for all $n \geq 1$.*

This has many consequences, a sample of which we list here. Many of these are of course well-known (see [3, Section 2.IV]) or follow easily from well-known congruences.

(a) Taking $n = p$ gives

$$L_p = F_{p-2} + 3F_{p-1} \equiv 1 \bmod p. \tag{7}$$

(b) It follows from (a) that

$$F_{p-1} \equiv 1 \bmod p \ \Leftrightarrow F_{p-2} \equiv -2 \bmod p, \tag{8}$$

which will be used below.

(c) Taking $n = p^k$ gives

$$L_{p^k} \equiv L_{p^{k-1}} \bmod p^k \tag{9}$$

for all primes p and $k \geq 1$.

(d) Taking $n = pq$ (a product of distinct primes) gives

$$L_{pq} + 1 \equiv L_p + L_q \bmod pq.$$

3. Obstruction

The negative part of Theorem 1 is proved as follows. Using some simple modular results on the Fibonacci numbers, we show that if the sequence (U_n) defined by (4) is exactly realizable, then the property (3) forces the congruence $b \equiv 3a \bmod p$ to hold for infinitely many primes p, so (U_n) is a multiple of (L_n).

Lemma 4. *For any prime p, $F_{p-1} \equiv 1 \bmod p$ if $p = 5m \pm 2$.*

Proof. From Hardy and Wright, [1, Theorem 180], we have that $F_{p+1} \equiv 0 \bmod p$ if $p = 5m \pm 2$. The identities $F_{p+1} = 2F_{p-1} + F_{p-2} \equiv 0 \bmod p$ and (7) imply that $F_{p-1} \equiv 1 \bmod p$. □

Assume now that the sequence (U_n) defined by (4) is exactly realizable. Applying (3) for n a prime p shows that

$$U_p - U_1 \equiv 0 \bmod p,$$

so by (5)

$$aF_{p-2} + bF_{p-1} \equiv a \bmod p.$$

If p is 2 or 3 mod 5, Lemma 4 then implies that

$$(F_{p-2} - 1)\, a + b \equiv 0 \bmod p. \tag{10}$$

On the other hand, for such p, (8) implies that $F_{p-2} \equiv -2 \bmod p$, so (10) gives

$$b \equiv 3a \bmod p.$$

By Dirichlet's theorem (or simpler arguments) there are infinitely many primes p with p equal to 2 or 3 mod 5, so $b \equiv 3a \bmod p$ for arbitrarily large values of p. We deduce that $b = 3a$, as required.

4. Remarks

(a) Notice that the example of the golden mean shift plays a vital role here. If it were not to hand, exhibiting a dynamical system with the required properties would require *proving* Corollary 3, and *a priori* we have no way of guessing or proving this congruence without using the dynamical system.

(b) The congruence (7) gives a different proof that $F_{p-1} \equiv 0$ or $1 \bmod p$ for $p \neq 2, 5$. If $F_{p-1} \equiv \alpha \bmod p$, then (7) shows that $F_{p-2} \equiv 1 - 3\alpha \bmod p$, so $F_p \equiv 1 - 2\alpha$. On the other hand, the recurrence relation gives the well-known equality

$$F_{p-2}F_p = F_{p-1}^2 + 1,$$

(since p is odd) so $1 - 5\alpha + 6\alpha^2 \equiv \alpha^2 + 1$, hence $5(\alpha^2 - \alpha) \equiv 0 \bmod p$. Since $p \neq 5$, this requires that $\alpha^2 \equiv \alpha \bmod p$ so $\alpha \equiv 0$ or 1.

(c) The general picture of conditions on linear recurrence sequences that allow exact realization is not clear, but a simple first step in the Fibonacci spirit is the following question. For each $k \geq 1$ define a

recurrence sequence $(U_n^{(k)})$ by

$$U_{n+k}^{(k)} = U_{n+k-1}^{(k)} + U_{n+k-2}^{(k)} + \cdots + U_n^{(k)}$$

with specified initial conditions $U_j^{(k)} = a_j$ for $1 \le j \le k$. The subshift of finite type associated to the $0-1$ $k \times k$ matrix

$$A^{(k)} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ & & \ddots & & & \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{bmatrix}$$

shows that the sequence $(U_n^{(k)})$ is exactly realizable if $a_j = 2^j - 1$ for $1 \le j \le k$. If the sequence is exactly realizable, does it follow that $a_j = C(2^j - 1)$ for $1 \le j \le k$ and some constant C? The special case $k = 1$ is trivial, and $k = 2$ is the argument above. Just as in Corollary 3, an infinite family of congruences follows for each of these multiple Fibonacci sequences from the existence of the exact realization.

References

[1] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, fifth edition, 1979.

[2] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, Cambridge, 1995.

[3] P. Ribenboim. *The New Book of Prime Number Records*. Springer, New York, 3rd edition, 1995.

[4] H.S. Wilf. *generatingfunctionology*. Academic Press, San Diego, 1994.

1991 *Mathematics Subject Classification.* 11B39, 58F20